EFFACTS DATA PROCESSING ADDENDUM

This Effacts Data Processing Addendum (this "**Addendum**") is effective as of May 25, 2018 ("**Addendum Effective Date**") and forms a part of the Effacts Service Terms and Conditions (the "**Terms and Conditions**") between CCH Incorporated, a Wolters Kluwer company ("**CCH**") and an individual, institution or organization ("**Customer**") subscribing to the Product pursuant to an order form or agreement (together with the Terms and Condition, and as may be amended from time to time, the "**Agreement**"). In the course of providing the Services (as defined below), CCH may process personal data (as defined below) on behalf of Customer, and CCH agrees to comply with the following provisions with respect to any such personal data.

1. Definitions. Capitalized terms used but not defined in this Addendum will have the same meanings as set forth in the Agreement. In this Addendum, the following terms shall have the meaning set out below:

a. "**Affiliate**" has the meaning given to such term in the Agreement.

b. "**Customer Personal Data**" means any personal data of a data subject that is processed by CCH on behalf of Customer to perform the Services under the Agreement.

c. "**control**" (or variants of it) means the ability, whether directly or indirectly, to direct the management and action of an entity by means of ownership, contract or otherwise.

d. "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including (with effect from May 25, 2018) by the GDPR and laws implementing, replacing or supplementing the GDPR.

e. "**EU Laws**" means European Union or Member State law, including EU Data Protection Laws.

f. "**GDPR**" means EU General Data Protection Regulation 2016/679.

g. "**Restricted Transfer**" means a transfer of Customer Personal Data from CCH to a Subprocessor where such transfer would be prohibited by EU Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of EU Data Protection Laws) in the absence of appropriate safeguards required for such transfers under EU Data Protection Laws.

h. "**Services**" means the Effacts Services, as well as all related services (such as Support services), provided to Customer by CCH pursuant to the Agreement.

i. "**Standard Contractual Clauses**" means the latest version of the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (the current version as at the date of this Addendum is annexed to European Commission Decision 2010/87/EU).

j. “**Subprocessor**” means any party (including CCH’s Affiliates and any other third parties) appointed by CCH to process Customer Personal Data to perform the Services.

k. The terms “**controller**”, “**data subject**”, “**personal data**”, “**personal data breach**”, “**processor**”, “**processing**”, and “**supervisory authority**” shall have the meanings ascribed to them in the GDPR, and their cognate terms shall be construed accordingly.

2. Customer Warranties. Customer warrants that:

a. Customer’s processing of the Customer Personal Data is based on legal grounds for processing as may be required by EU Data Protection Laws and it has made and shall maintain throughout the term of the Agreement all necessary rights, permissions, registrations and consents in accordance with and as required by EU Data Protection Laws with respect to CCH’s processing of Customer Personal Data under this Addendum and the Agreement; and

b. It is entitled to and has all necessary rights, permissions and consents to transfer the Customer Personal Data to CCH and otherwise permit CCH to process the Customer Personal Data on its behalf, so that CCH may lawfully use, process and transfer the Customer Personal Data in order to carry out the Services and perform CCH’s other rights and obligations under this Addendum and the Agreement.

3. Controller and Processor. For purposes of this Addendum, Customer is the controller of the Customer Personal Data and CCH is the processor of such data, except when Customer acts as a processor of Customer Personal Data, in which case CCH is a subprocessor. Customer and its Affiliates, as their respective controllers, shall determine the purposes of collecting and processing Customer Personal Data.

4. Scope of Processing.

a. In order for CCH to provide the Services under the Agreement, CCH will process Customer Personal Data. Annex 1 to this Addendum sets out certain information regarding the processing of Customer Personal Data as required by Article 28(3) of the GDPR. The parties may amend Annex 1 from time to time as the parties may reasonably consider necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this Section 4(a)) confers any right or imposes any obligation on any party to this Addendum.

b. CCH shall only process Customer Personal Data (i) in accordance with the documented instructions described in this Addendum, and (ii) for the purposes of fulfilling its obligations under the Agreement. If EU Law to which CCH is subject requires CCH to process Customer Personal Data in a manner contrary to Customer’s instructions, CCH shall inform Customer in advance of any relevant processing of the affected Customer Personal Data, unless the relevant EU Law prohibits this on important grounds of public interest.

c. CCH shall inform Customer if, in CCH’s opinion, an instruction given by Customer under this Section 4 infringes EU Law. CCH shall have the right to suspend processing of Customer Personal Data until Customer’s instruction is clarified to the extent that it no longer infringes EU Law.

5. Confidentiality. CCH shall ensure that each of its personnel that is authorized to process Customer Personal Data is subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

6. Security.

a. CCH shall, in relation to Customer Personal Data, (a) take, as appropriate, measures required pursuant to Article 32 of the GDPR, and (b) on reasonable request at Customer's cost, assist Customer in ensuring compliance with Customer's obligations pursuant to Article 32 of the GDPR, taking into account the nature of the processing and the information available to CCH.

b. CCH shall maintain the security practices and policies for the protection of Customer Personal Data as set forth in Annex 2 of this Addendum. Customer warrants that it has assessed the security measures set out in Annex 2 of this Addendum and has determined that they satisfy the requirements of Article 32 GDPR in respect of CCH's processing of Customer Personal Data.

7. Subprocessors. Customer hereby authorizes CCH to appoint Subprocessors in accordance with this Section 7, subject to any restrictions in the Agreement. CCH will bind Subprocessors with written agreements that require them to provide at least the level of data protection required of CCH by this Addendum relative to the Subprocessor's activities relating to the Services. Customer authorizes CCH's engagement of CCH's Affiliates, and the third party(ies) listed in Annex 1, as Subprocessors. In case CCH intends to engage new or additional Subprocessors, CCH will inform Customer in writing (which may be by email or other Product-enabled notification to Customer's Product Administrator) of such additions or replacements (the "**Subprocessor Notice**"). If Customer has reasonable grounds proving that significant risks for the protection of its Customer Personal Data exist with such new or additional Subprocessor(s), Customer will notify CCH in writing within 30 days of the date of the Subprocessor Notice, detailing the basis for the objection. CCH will work with Customer in good faith to make available a commercially reasonable change in the provision of the Services or recommend a commercially reasonable change to such Customer's configuration or use of the Services to avoid processing of Customer Personal Data by the objected-to new or additional Subprocessor(s) without unreasonably burdening Customer, in either case which avoids the use of the Subprocessor(s). Where such a change cannot be made within 90 days from CCH's receipt of Customer's objection notice, notwithstanding anything in the Agreement, Customer, may, as its sole remedy, by written notice to CCH with immediate effect terminate that portion of the Agreement that relates to the Services that require the use of such new or additional Processor. CCH shall be responsible for the acts and omissions of any Subprocessors as it is to Customer for its own acts and omissions in relation to the matters provided in this Addendum. The provisions of this Section 7 shall not apply to the extent Customer instructs CCH to allow a third party to Process Customer Personal Data pursuant to a contract that Customer has directly with the third party.

8. Data Subject Requests. To the extent legally permitted, CCH will promptly notify Customer if CCH or any Subprocessor receives any complaint, inquiry or request (including requests made by data subjects to exercise their rights pursuant to EU Data Protection Laws) related to Customer Personal Data. Taking into account the nature of the processing, CCH shall assist Customer at Customer's cost and request, by appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfillment of Customer's obligation to respond to requests for exercising such data subjects' rights.

9. Data Breach. CCH shall notify Customer without undue delay once CCH becomes aware of a personal data breach affecting Customer Personal Data. CCH shall, taking into account the nature of the processing and the information available to CCH, use commercially reasonable efforts to provide Customer with sufficient information to allow Customer, at Customer's cost, to meet any obligations to notify or inform regulatory authorities, data subjects and other entities of such personal data breach to the extent required under EU Data Protection Laws.

10. Data Protection Impact Assessments. CCH shall, taking into account the nature of the processing and the information available to CCH, provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments and prior consultations with supervisory authorities or other competent regulatory authorities as required for Customer to fulfill its obligations under EU Data Protection Laws.

11. Destruction of Customer Personal Data.

a. Subject to Section 11.b. below, or as otherwise required by applicable law, CCH will promptly and in any event by the later of: (i) 90 days after the date of cessation of any Services involving the processing of Customer Personal Data; (ii) termination of the Agreement, and (iii) expiration of the time period for which Customer Personal Data is maintained pursuant to applicable disaster recovery practices for the Services, to the extent reasonably practicable, delete and procure the deletion of all copies of Customer Personal Data processed by CCH. For the avoidance of doubt, CCH may retain Customer Personal Data as required by EU Laws.

b. For so long as CCH and each Subprocessor retains Customer Personal Data in accordance with this Section 11, CCH's obligations of confidentiality with respect to such Customer Personal Data will continue and CCH will ensure that such Customer Personal Data is only processed as necessary and for no other purpose.

12. Audit.

a. Subject to Sections 12(b) and (c), CCH shall make available to Customer upon reasonable written request, information that is reasonably necessary to demonstrate CCH's compliance with this Addendum. Customer shall be responsible for any costs and expenses of CCH arising from the provision of such information and audit rights.

b. Customer's information and audit rights only arise under Section 12(a) above to the extent that the Agreement and/or any other information available to Customer in relation to the Services does not otherwise give Customer information and audit rights meeting the requirements of Section 12(a) above.

c. Customer is aware that any in-person on-site audits are likely to significantly disturb CCH's business operations, including operations relating to the Services being provided pursuant to the Agreement. Customer shall ensure that its auditors make reasonable efforts to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to CCH's premises, equipment, personnel and business while its auditor personnel are on those premises in the course of such an audit or inspection. Each requested audit shall meet the following requirements:

   i. no more than one audit per calendar year shall be requested or conducted and upon no less than 90 days' notice to CCH;

ii. shall be conducted by an internationally recognized independent auditing firm reasonably acceptable to CCH;

iii. take place during CCH's regular business hours, pursuant to a mutually agreed upon scope of audit;

iv. the duration of the audit must be reasonable and in any event shall not exceed two business days;

v. no access shall be given to the data of other customers; audits will not be permitted if they interfere with CCH's ability to provide the Services to any customers;

vi. audits shall be subject to any confidentiality or other contractual obligations of CCH or CCH's Affiliates (including any confidentiality obligations to other customers, vendors or other third parties);

vii. any non-affiliated third parties participating in the audit shall execute a confidentiality agreement reasonably acceptable to CCH;

viii. all costs and expenses of any audit shall be borne by Customer; and

ix. any audit of a facility will be conducted as an escorted and structured walkthrough and shall be subject to CCH's security policies.

d. CCH shall immediately inform Customer if, in CCH's opinion, an instruction in relation to Customer's rights under this Section 12 infringes EU Law. CCH shall have the right to suspend processing of Customer Personal Data until Customer's instruction is clarified to the extent that it no longer infringes EU Law.

13. Data Transfer.

CCH and Customer hereby enter into the Standard Contractual Clauses in the form set forth in Annex 3 in respect of any Restricted Transfer. If CCH's arrangement with a Subprocessor involves a Restricted Transfer, CCH shall incorporate the onward transfer provisions of the Standard Contractual Clauses into the agreement entered into between CCH (who shall be permitted to enter the Standard Contractual Clauses on behalf of Customer) and the Subprocessor or, if the Subprocessor is Privacy Shield certified or operating under binding corporate rules, a requirement that the Subprocessor maintain its Privacy Shield certification or binding corporate rules, as applicable, throughout the term of the Agreement. Customer agrees to exercise its audit right in the Standard Contractual Clauses by instructing CCH to conduct the audit set out in Section 12.

14. Miscellaneous.

a. Except as otherwise set forth herein, all terms and conditions of the Agreement will continue in full force and effect as set forth therein and amended thereby. Nothing in this Addendum reduces CCH's obligations under the Agreement in relation to the protection of Customer Personal Data or permits CCH to process (or permit the processing of) Customer Personal Data in a manner that is prohibited by the Agreement.

b. Notwithstanding any terms of the Agreement to the contrary, in the event and to the extent of any conflict between the terms and conditions of (i) this Addendum and applicable law, the provision(s) of the applicable law shall govern; (ii) this Addendum and the Standard Contractual Clauses, the provision(s) of the Standard Contractual Clauses shall govern; and (iii) this Addendum and the Agreement, the provision(s) that are more protective of Customer Personal Data shall govern. CCH shall comply with the terms of this Addendum during the term of the Agreement and during any period during which CCH may have access to Personal Data.

c. CCH may modify or supplement this Addendum, with reasonable notice to Customer:

i. If required to do so by a supervisory authority or other government or regulatory entity;

ii. If necessary to comply with applicable law;

iii. To implement new or updated Standard Contractual Clauses approved by the European Commission; or

iv. To adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 GDPR.

d. Without prejudice to Clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses, this Addendum will be governed by the laws of the country or territory stipulated in the Agreement.

e. Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

[End of Addendum; Annexes follow]

ANNEX 1

DETAILS OF PROCESSING OF PERSONAL DATA

This Annex includes certain details of the processing of Personal Data:

Subject matter and duration of the processing of Personal Data

This Addendum addresses the processing of Customer Personal Data in connection with Customer's subscription to, and CCH's hosting and provision of, the Effacts online service (a software-as-a service application) pursuant to the terms of the Agreement. Effacts is an information and document repository of organization legal information, such as that relating to key contracts, other documents, policies, claims, legal entities and intellectual property and other organization information. CCH will process the Customer Personal Data during the term of the Agreement (including any renewal) and until the later of: (i) 90 days after the date of cessation of any Services involving the processing of Customer Personal Data, (ii) the expiration of any continuing obligations of CCH to retain Customer Personal Data under the Agreement, and (iii) the expiration of the time period for which Customer Personal Data is maintained pursuant to applicable disaster recovery practices for the Services.

The nature and purpose of the processing of Personal Data

CCH will process Customer Personal Data as necessary to perform the Services and fulfill Customer's subscription to the Effacts Service, as further instructed by Customer, and including:

- For the operation, maintenance and development of the Effacts Service,
- For providing Services related to the inherent functionality of the Effacts Service,
- For hosting the Product,
- For implementation services,
- For Support, and
- For providing Services relating to the availability of the Customer Personal Data (such as disaster recovery purposes).

The types of Personal Data to be processed

Customer may input Customer Personal Data into the Effacts Service or otherwise provide Customer Personal Data in connection with its subscription to the Effacts Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include the following categories of Personal Data:

- First and last names of natural persons
- Titles
- Contact information (including home and work street and email addresses and telephone numbers)
- Marital status and gender

- Citizenship information
- Governmental identification information, including drivers' license information, passport information
- Professional life data, including photographs
- Related person's data

The categories of data subject to whom the Personal Data relates

Customer may input Customer Personal Data into the Effacts Service or otherwise provide Customer Personal Data in connection with its subscription to the Effacts Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include information with respect to the following categories of data subjects: employees, independent contractors, officers, directors, advisors, parties and counter-parties to contracts, claimants, and vendors.

List of current Subprocessors:

- Amazon Web Services (hosting provider, United States of America)
- Twilio (two-factor authentication, California, United States of America)
- Wolters Kluwer N.V. affiliates, including Wolters Kluwer Tech B.V. (Netherlands), Wolters Kluwer Italy, Kluwer Netherlands (development, support and other software application and related services)

ANNEX 2

INFORMATION SECURITY

CCH currently maintains the security practices with respect to its Effacts software as a service product that are described in this Annex 2. Notwithstanding any provision to the contrary, CCH may update or change these security practices from time to time at its discretion however CCH will not materially diminish the overall level of security measures without notifying Effacts customers. The U.S. instance of Effacts is currently hosted on Amazon Elastic Compute Cloud (Amazon EC2) (https://aws.amazon.com/it/ec2/details/).

The Effacts service security program is designed to (i) maintain the availability of the Effacts services and its systems and customer information, (ii) control access to the Effacts services and its systems and customer information, and (iii) maintain the confidentiality and integrity of customer information within the Effacts service. Mechanisms of the information security program include the governance risk and compliance teams within IT-Security, risk management, including vendor risk review, logging and monitoring, internal and external audits/assessments, internal controls assessment, internal and external penetration and vulnerability assessments, contract management, security awareness, security consulting and policy exception reviews. More specifically, the Effacts service security program is comprised of the following:

1. Policies and Risk Assessment. CCH has implemented an Information Security Policy that encompasses a variety of policies for managing information and technology assets intended to protect underlying applications and data. Policies are reviewed on a periodic basis. Information security risk assessments are also conducted on a periodic basis.

2. Human Resources. U.S. based Effacts employees undergo background checks and participate in security awareness training on a regular basis.

3. Effacts Infrastructure & Role Separation. Resources that support infrastructure and application services are delineated access privileges based on job responsibilities limiting access privileges to that necessary to perform responsibilities. Infrastructure credentialing requires management approval and business processes are implemented to periodically review level of privileges and address changes in role, privilege revocation and termination. CCH implements minimum standard password policy addressing complexity, age and history of password controls.

4. Customer Credential Management. Application credentials are managed by customers.

5. Data Protection. Customer data is encrypted in transit and at rest on production servers. Unique data keys are generated for each customer. Customer data is backed up daily and backups are kept for 30 days. Data is destroyed using secured techniques.

6. Environment Separation. Effacts maintains physical and/or logical environment separation for the effacts.com application, including separate development, testing, staging and production environments. The production application is hosted on Amazon Elastic Compute Cloud (Amazon EC2), https://aws.amazon.com/it/ec2/details/, which includes access controls, onsite security, fire

suppression, uninterruptable power supply, backup generators, redundant pathways, components, power and cooling systems.

7. Availability. The computing components are deployed with one or more redundant backups in a high available environment configuration (in separate data centers), which includes a disaster recovery environment. Health and performance monitoring is conducted on all computing systems. Capacity planning is periodically assessed.

8. Operations Management. CCH maintains release management, change management, incident management and security management processes. CCH tracks key performance metrics.

9. Vulnerability and Penetration Testing. CCH conducts internal and external vulnerability and penetration testing of the Effacts application and infrastructure on a periodic basis.

ANNEX 3

STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

The data exporter is: The subscribing customer to Effacts online service (or an affiliate of such customer, if applicable):

And

The data importer is: CCH Incorporated, 2700 Lake Cook Road, Riverwoods, Illinois 60015

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter, or one of its affiliates, has entered into a data processing addendum (“DPA”) with the data importer, or one of its affiliates. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer, or one of its affiliates, as applicable, will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter

The data exporter is: The subscribing Customer to Effacts online service (or an affiliate of such customer, if applicable)

Data importer

The data importer is: CCH Incorporated, 2700 Lake Cook Road, Riverwoods, Illinois 60015

Data subjects

The personal data transferred concern the following categories of data subjects:

Customer may input Customer Personal Data into the Effacts Service or otherwise provide Customer Personal Data in connection with its subscription to the Effacts Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include information with respect to the following categories of data subjects: employees, independent contractors, officers, directors, advisors, parties and counter-parties to contracts, claimants, and vendors.

Categories of data

The personal data transferred concern the following categories of data:

Customer may input Customer Personal Data into the Effacts Service or otherwise provide Customer Personal Data in connection with its subscription to the Effacts Service, the extent of which is determined and controlled by Customer in its sole discretion but which may include the following categories of Personal Data:

- First and last names of natural persons
- Titles
- Contact information (including home and work street and email addresses and telephone numbers)
- Marital status and gender
- Citizenship information
- Governmental identification information, including drivers' license information, passport information
- Professional life data, including photographs
- Related person's data

Special categories of data (if appropriate)

Use of the Effacts Service doesn't anticipate the transfer of special categories of data.

Processing operations

The personal data transferred will be subject to the following basic processing activities:

CCH will process Customer Personal Data as necessary to perform the Services and fulfill Customer's subscription to the Effacts Service, as further instructed by Customer, and including:

- For the operation, maintenance and Development of the Effacts Service,
- For providing Services related to the inherent functionality of the Effacts Service,
- For hosting the Product,
- For implementation services,
- For Support, and
- For providing Services relating to the availability of the Customer Personal Data (such as disaster recovery purposes).